



Delaware Cyber Security Advisory Council



State of Delaware
Delaware Cyber Security Advisory Council Meeting Minutes
March, 23, 2016

Cyber Security Advisory Council Attendees

Name	Organization	Attendance	Designee in attendance
James Collins	CIO, State of Delaware	Present	
Joshua Brechbuehl	IT Manager, City of Newark	Excused	Diana Montgomery
Jason Christman	Lt. Colonel, Delaware National Guard	Present	
Richard Gowan	Network Security Principal Engineer, Verizon	Present	
Mike Maksymow	CIO, Beebe Healthcare	Present	
Daniel Meadows	Captain, Delaware State Police	Present	
Doug Myers	CIO, Pepco Holdings, Inc.	Present	
Bruce Patrick	VP & General Manager, Tidewater Utilities, Inc.	Present	
Dr. Marwan Rasamny	Department Chair, Delaware State University	Present	
Diane Rogerson	Technology Managing Director, JP Morgan Chase	Present	
AJ Schall, Director	Delaware Emergency Management Agency	Present	
Elayne Starkey	CSO, State of Delaware	Present	

Call to Order

Chief Information Officer James Collins called the first Delaware Cyber Security Advisory Council (CSAC) meeting to order at approximately 9:10 am on March 23, 2016.

Welcome

Governor Jack Markell welcomed everyone and invited the council to introduce themselves. Others in attendance: Lisa Morris, DOJ; Claudette Martin-Wus, DTI; Agent Daniel Gray, FBI; Sandra Alexander, DTI; Trevor Fulmer, National Guard; Mark Grubb, Division of Communications; Mike Hojnicky, DTI; Raymond Holcomb, DSHS; Parthiban Jayaraman, DTI; Bonnie Metz, Verizon; Aleine Porterfield, DOJ; Randall Chase, Associated Press; and Joe Irzarry, WCDE News.

Governor Markell applauded the balance and expertise of the Council. He emphasized the importance of “getting this right” and asked the Council to be proactive in its recommendations for a coordinated focus to achieve a high level of cyber resiliency across all sectors in Delaware. Let’s “check our egos at the door” and identify what we can share. The Governor added he doesn't expect anyone to divulge company secrets or protected information.

CIO James Collins reported that last year there were over 1,500 cyber attacks across the globe, resulting in billions of stolen records. The CSAC is designed to drive efforts of prevention and risk mitigation, as well to create a stewardship for information. He added that “we all have an obligation to protect information by any means necessary.”

Meeting Logistics

One of DTI's goals is for the CSAC to operate in a paperless environment as much as possible. Claudette Martin-Wus introduced eBoard, a platform for meeting documents, including agendas, presentations, and minutes of the Council. Martin-Wus described the features of eBoard, emphasizing DTI's cloud security vetting and the difference between open items and confidential items.

Lisa Morris from the Department of Justice discussed Delaware's Open Meeting Law and Freedom of Information Act (FOIA), which governs this Council. The purpose of FOIA is to give citizens access to government proceedings and increase government transparency. Citizens can access Public Meeting documents through the state portal. The public is welcome to attend CSAC meetings and DTI has a responsibility to give seven (7) days advance notice. The Council can vote to go into Executive Session, which would include necessary board members, their staff, and attorneys. Voting may only be held during public portion of the meeting. Minutes for both the public meetings and Executive Sessions are required. The minutes for the Executive Session are kept separate and have restrictions on distribution.

A public meeting requires a quorum to convene. CSAC has 12 council members, thus the quorum is 7. Video conferencing does not count toward the quorum unless the video conference site is open to the public. Council members appointed by the Governor may not send a designee. Council members appointed by title may send a designee, but the same person is preferred for consistency.

Executive Order 55

CSO Elayne Starkey reported that this Council was created by Governor Markell's Executive Order 55 to be the central interface for coordinating cyber security initiatives among the public and private sectors. We have been asked to facilitate cross-industry collaboration to share best practices and mitigate cyber risks related to critical infrastructure. Our specific directive, as spelled out in the Executive Order is to develop recommendations in 3 areas:

- 1) for improving the overall cyber security posture across all sectors in Delaware
- 2) for increasing information sharing between all sectors in Delaware
- 3) resources (funding, people) and possible methods to accomplish

We are ultimately accountable to the Governor and will report on our activities and recommendations to the Governor's Office at least once a year. We may also report out to the Delaware Homeland Security Advisory Council

The genesis of this Council is the Delaware Information Sharing and Analysis Center Steering Committee, comprised of Department of Safety and Homeland Security, State Police, National Guard, and DTI.

Elayne proposed that the CSAC convene initially every 4-6 weeks as we discuss and prepare our roadmap. An email distribution list has been established for easy communication and notification among the CSAC Members. As we grow, spinoff subcommittees may be created to encompass other aspects of these goals and report back to the council.

CIO Collins stated the CSAC will feed into what other agencies like DEMA are doing and not work as a separate function from them.

Unclassified FBI Threat Briefing

SSA Daniel Gray, FBI, introduced his cyber security threat briefing by describing how at-risk our local and state governments and utilities are to terrorist/cyber attacks. With more convenience comes less security, and vice versa. Agent Gray stated that hackers look to identify users and target behaviors through tactics such as spear phishing. Malware is growing in complexity. Hackers and cyber criminals are targeting mobile devices, laptops, tablets; and are increasing their recruitment of insiders through various means.

The balance of the presentation included tactical and response practices and procedures currently employed by the FBI. Because of the concern that public disclosure of this information would constitute an endangerment to state and national security, a motion to amend the agenda to include an Executive Session and move to an Executive Session per 29 Del. C. §§ 10002(l)(5), 10004(b)(6), & 10004(e)(2) was called. AJ Schall moved. Mike Maksymow seconded. Ayes had the majority.

FOIA Proposal

The current Delaware Freedom of Information Act (FOIA) includes exclusions that focus primarily on physical security protection rather than cyber security protection. Examples of things we protect now are emergency response plans, building blueprints, and alarm system schematics. Although “telecommunications networks facilities and switching equipment” is also listed, we are recommending that the code be broadened to include exclusions for computer system architecture and schematics, system source code, data dictionaries, record layouts, and system and network architecture diagrams. The release of information about the underpinnings of our state computer network and systems would introduce a very serious security risk. This data in the hands of a nefarious requestor gives them an advantage when attempting to break into our systems to steal data about our citizens, in the same way that blueprint and alarm data helps someone attempting physical harm. DTI is working with the attorneys to put together proposed legislation for discussion at the next Council meeting.

Next Meetings

Proposed dates for the next three CSAC meetings in Dover are:

Wednesday April 27 9:30 AM

Wednesday June 29 9:00 AM

Wednesday, August 31 9:00 AM

Homework assignment: Consider ideas to address our specific directives, as spelled out in the Executive Order. Discuss with your team. Bring your recommendations to the next meeting.

- 1) improve the overall cyber security posture across all sectors in Delaware
- 2) increase information sharing between all sectors in Delaware
- 3) identify resources (funding, people) and possible methods to accomplish

Other Business

AJ Schall requested an overview of the statewide cyber security exercise held last October.

Mike Maksymow suggested creating a separate body of healthcare representation. He also inquired what is appropriate to share outside of the council. CIO Collins answered that everything, aside from Executive Sessions, can be shared outside of the council.

Public Comment

There was no public comment.

Adjournment

James Collins thanked the council for a successful kick-off of the CSAC and entertained a motion to adjourn. With no further business to be conducted, Daniel Meadows made the motion to adjourn, and AJ Schall seconded the motion. With no opposition, the motion was carried. The meeting was adjourned at approximately 11:16 am.

Respectfully submitted,
Ronda Ramsburg
Deborah Hawkins